COVER SHEET FOR AMENDMENT OF POST-TRAVEL SUBMISSION

Instructions: Use this form as a cover sheet for any paperwork you may need to submit to the **Office of Public Records** in order to make your Privately Sponsored Post-Travel Submission complete in accordance with Rule 35. **Only complete this form if you need to submit an amendment to a post-travel filing you have already submitted.**

SUBMIT DIRECTLY TO THE OFFICE OF PUBLIC RECORDS IN 232 HART BUILDING

Name of Traveler: Clint Trocchio

Employing Office/Committee: U.S. Senate Committee on Appropriations

Travel Expenses Paid by (List all sources): Stanford University

Travel Date(s): August 26-31, 2019

Description/Title of Attached Forms: Form RE-2 (attached); the final version of the Private Sponsor Travel Certification Form; and the final version of your personalized itinerary

Purpose of Amendment (describe the reason for amending original submission): Corrections to Form RE-2 (attached); the final version of the Private Sponsor Travel Certification Form; and the final version of your personalized itinerary

9.27.19
(Date)

(Signature of Traveler)

(Revised 4/19/2010)

Employee Post-Travel Disclosure of Travel Expenses

Post-Travel Filing Instructions: Complete this form within **30 days** of returning from travel. Submit all forms to the **Office of Public Records in 232 Hart Building.**

In compliance with Rule 35.2(a) and (c), I make the following disclosures with respect to travel expenses that have been or will be reimbursed/paid for me. I also certify that I have attached:

☒ The **original** *Employee Pre-Travel Authorization* (Form RE-1), **AND**
☒ A **copy** of the *Private Sponsor Travel Certification Form* with all attachments (itinerary, invitee list, etc.)

Private Sponsor(s) (list all): Stanford University

Travel date(s): August 26-29, 2019

Name of accompanying family member (if any): N/A
Relationship to Traveler: ☐ Spouse   ☐ Child

IF THE COST OF LODGING **DID NOT INCREASE** DUE TO THE ACCOMPANYING SPOUSE OR DEPENDENT CHILD, ONLY INCLUDE LODGING COSTS IN EMPLOYEE EXPENSES. (Attach additional pages if necessary.)

Expenses for Employee:

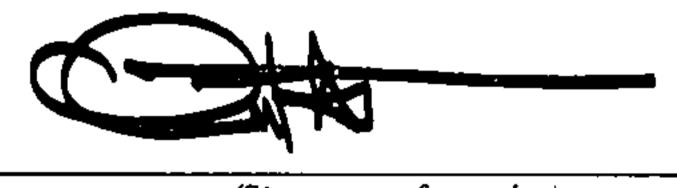|	Transportation Expenses	Lodging Expenses	Meal Expenses	Other Expenses (Amount & Description)
☐ Good Faith Estimate ☐ Actual Amount	599.45	$600 ($200/night)	$191.07	$86.68 CA ground transportation

Expenses for Accompanying Spouse or Dependent Child (if applicable):

	Transportation Expenses	Lodging Expenses	Meal Expenses	Other Expenses (Amount & Description)
☐ Good Faith Estimate ☐ Actual Amount	N/A	N/A	N/A	N/A

Provide a description of all meetings and events attended. *See* Senate Rule 35.2(c)(6). (Attach additional pages if necessary.): See attached itinerary.

9.27.19	Clinton A. Trouhio	[signature]
(Date)	*(Printed name of traveler)*	*(Signature of traveler)*

TO BE COMPLETED BY SUPERVISING MEMBER/OFFICER:

I have made a determination that the expenses set out above in connections with travel described in the *Employee Pre-Travel Authorization* form, are necessary transportation, lodging, and related expenses as defined in Rule 35.

10/11/19	Richard Shelby [signature]
(Date)	*(Signature of Supervising Senator/Officer)*

(Revised 1/3/11)   Form RE-2

PRIVATE SPONSOR TRAVEL CERTIFICATION FORM

This form must be completed by any private entity offering to provide travel or reimbursement for travel to Senate Members, officers, or employees (Senate Rule 35, clause 2). Each sponsor of a fact-finding trip must sign the completed form. The trip sponsor(s) must provide a copy of the completed form to each invited Senate traveler, who will then forward it to the Ethics Committee with any other required materials. The trip sponsor(s) should **NOT** submit the form directly to the Ethics Committee. Please consult the accompanying instructions for more detailed definitions and other key information.
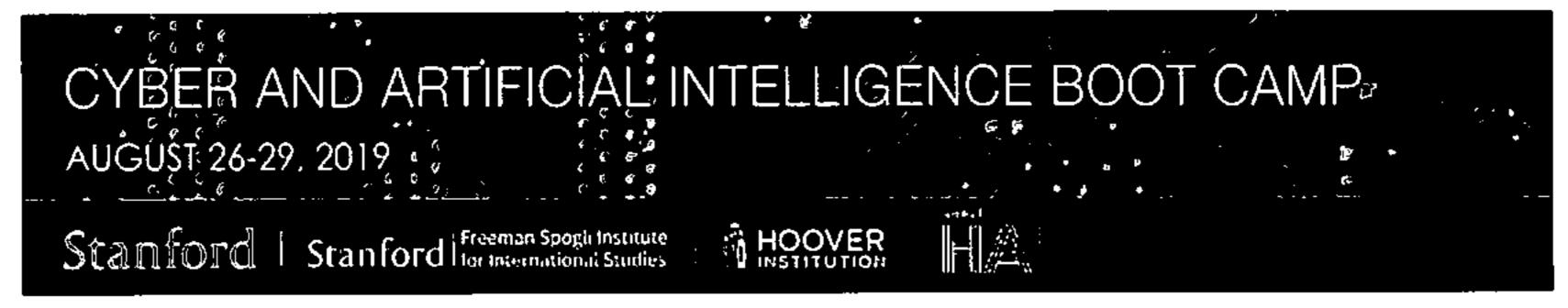
The Senate Member, officer, or employee **MUST** also provide a copy of this form, along with the appropriate travel authorization and reimbursement form, to the Office of Public Records (OPR), Room 232 of the Hart Building, within thirty (30) days after the travel is completed.

1. Sponsor(s) of the trip (please list all sponsors): Stanford University (Partnership between Stanford's Hoover Institution, Freeman Spogli Institute, Human Centered Artificial Intelligence Institute)

2. Description of the trip: An intensive program for Congressional staff which consists of three days of seminars, simulations, and keynote presentations.

3. Dates of travel: August 26 - 29, 2019

4. Place of travel: Stanford University, Stanford, CA

5. Name and title of Senate invitees: See attached list

6. I *certify* that the trip fits one of the following categories:

   ☐ (A) The sponsor(s) are not registered lobbyists or agents of a foreign principal **and** do not retain or employ registered lobbyists or agents of a foreign principal **and** no lobbyist or agents of a foreign principal will accompany the Member, officer, or employee *at any point* throughout the trip.

   – OR –

   ☒ (B) The sponsor or sponsors are not registered lobbyists or agents of a foreign principal, but retain or employ one or more registered lobbyists or agents of a foreign principal and the trip meets the requirements of Senate Rule 35.2(a)(2)(A)(i) or (ii) *(see question 9)*.

7. ☒ I *certify* that the trip will not be financed in any part by a registered lobbyist or agent of a foreign principal.

   – AND –

   ☒ I *certify* that the sponsor or sponsors will not accept funds or in-kind contributions earmarked directly or indirectly for the purpose of financing this specific trip from a registered lobbyist or agent of a foreign principal or from a private entity that retains or employs one or more registered lobbyists or agents of a foreign principal.

8. I *certify* that:

   ☒ The trip will not in any part be planned, organized, requested, or arranged by a registered lobbyist or agent of a foreign principal except for *de minimis* lobbyist involvement.

   – AND –

   ☒ The traveler will not be accompanied on the trip by a registered lobbyist or agent of a foreign principal except as provided for by Committee regulations relating to lobbyist accompaniment *(see question 9)*.

Private Sponsor Certification - Page 1 of 4

9. **USE ONLY IF YOU CHECKED QUESTION 6(B)**

I *certify* that if the sponsor or sponsors retain or employ one or more registered lobbyists or agents of a foreign principal, one of the following scenarios applies:

☐ (A) The trip is for attendance or participation in a one-day event (exclusive of travel time and one overnight stay) and no registered lobbyists or agents of a foreign principal will accompany the Member, officer, or employee *on any segment* of the trip.

– OR –

☐ (B) The trip is for attendance or participation in a one-day event (exclusive of travel time and two overnight stays) and no registered lobbyists or agents of a foreign principal will accompany the Member, officer, or employee *on any segment* of the trip (*see questions 6 and 10).*

– OR –

☒ (C) The trip is being sponsored only by an organization or organizations designated under § 501(c)(3) of the Internal Revenue Code of 1986 and no registered lobbyists or agents of a foreign principal will accompany the Member, officer, or employee *at any point* throughout the trip.

10. **USE ONLY IF YOU CHECKED QUESTION 9(B)**

If the trip includes two overnight stays, please explain why the second night is practically required for Senate invitees to participate in the travel:

_____

_____

_____

11. ☒ An itinerary for the trip is attached to this form. I *certify* that the attached itinerary is a detailed (hour-by-hour), complete, and final itinerary for the trip.

12. Briefly describe the role of each sponsor in organizing and conducting the trip:

Stanford University soley planned all aspects of the trip including topics discussed, travel/accommodation

logistics, and required paperwork. Stanford staff will also be responsible for traveling with Congressional

staff and managing logistics for the duration of the trip.

13. Briefly describe the stated mission of each sponsor and how the purpose of the trip relates to that mission:

Stanford University is a 501(C)3 institution of higher education that seeks to promote the public welfare by

excercising an influence in behalf of humanity and civilization, through teaching and rigorous scholarship.

14. Briefly describe each sponsor's prior history of sponsoring congressional trips:

Stanford University has sponsored several trips for Congressional staff. Specifically, this is the fourth

Cyber Boot Camp for Congressional staff organized by Stanford. The most recent one was August 2017

and had a similar format to this trip.

15. Briefly describe the educational activities performed by each sponsor (other than sponsoring congressional trips):

Stanford University regularly sponsors policy panels and roundtables for think tank scholars, journalists,

Congressional staff, Executive branch officials, academics and members of the public. Additionally

Stanford educates numerous undergrad and graduate students within the university.

16. Total Expenses for Each Participant:

	Transportation Expenses	Lodging Expenses	Meal Expenses	Other Expenses
☒ Good Faith estimate ☐ Actual Amounts	$599.45 Round trip airfare $60 Ground transportation $659.45 Total	$600 ($200/night)	$218	None

17. State whether a) the trip involves an event that is arranged or organized *without regard* to congressional participation or b) the trip involves an event that is arranged or organized *specifically with regard* to congressional participation:

This trip involves an event that is arranged/organized specifically with regard to Congressional staff

participation.

18. Reason for selecting the location of the event or trip

IN order to have a significant number of California-based faculty participate in the event, we are hosting

it at the Stanford University campus.

19. Name and location of hotel or other lodging facility:

Schwab Residential Center, 680 Serra Street, Stanford CA 94305

20. Reason(s) for selecting hotel or other lodging facility:

The Schwab Residential Center is owned and operated by Stanford University. It is in close proximity to

the events that compromise the program, and falls into the per diem guidelines.

21. Describe how the daily expenses for lodging, meals, and other expenses provided to trip participants compares to the maximum per diem rates for official Federal Government travel:

Lodging expenses are less than the federal per diem for Stanford, CA. Meal expenses are less than the

federal per diem for Stanford, CA.

22. Describe the type and class of transportation being provided. Indicate whether coach, business-class or first class transportation will be provided. If first-class fare is being provided, please explain why first-class travel is necessary:

Stanford University will provide economy class round trip airfare between Washington, DC and San

Francisco, CA, and ground transportation in California.

23. ☒ I represent that the travel expenses that will be paid for or reimbursed to Senate invitees do not include expenditures for recreational activities, alcohol, or entertainment (other than entertainment provided to all attendees as an integral part of the event, as permissible under Senate Rule 35).

24. List any entertainment that will be provided to, paid for, or reimbursed to Senate invitees and explain why the entertainment is an integral part of the event:

None

25. I hereby *certify* that the information contained herein is true, complete and correct. (For trips involving more than one sponsor, you *must* include a completed signature page for each additional sponsor):

Signature of Travel Sponsor:

Name and Title: Russell Wald, Senior Manager, External Affairs

Name of Organization: Stanford University

Address: 434 Galvez Mall, Stanford, CA 94305

Telephone Number: 202.760.3200

Fax Number: 202.760.3191

E-mail Address: rwald@stanford.edu

Cyber and Artificial Intelligence Boot Camp
August 26-29, 2019

The Hoover Institution, Annenberg Conference Room 105, Lou Henry Hoover Building
434 Galvez Mall, Stanford, CA 94305

LEADERSHIP

Andrew Grotto
Program Director, Program on Geopolitics, Technology, and Governance, Stanford Cyber Policy Center, Freeman Spogli Institute
William J. Perry International Security Fellow, Center for International Security and Cooperation (CISAC)
Research Fellow, Hoover Institution
Dr. Herb Lin
Senior Research Scholar for Cyber Policy and Security, Center for International Security and Cooperation (CISAC)
Hank J. Holland Fellow in Cyber Policy and Security, Hoover Institution
Chief Scientist Emeritus, Computer Science and Telecommunications Board, National Academies

CONTACTS

Danielle Jablanski, djablanski@stanford.edu +1(650) 725-4839
Cyber Program Manager, Program on Geopolitics, Technology, and Governance, Stanford Cyber Policy Center, Freeman Spogli Institute
Russell Wald, rwald@stanford.edu +1 (202) 760-3204
Senior Manager for External Affairs
Hoover Institution, Stanford University

DAY 1 (Monday, August 26): Cyber Offense and Defense

9:49 a.m. - Arrive on Group Flight: United Airlines 1881 to San Francisco International Airport

---

11:30 am – 12:00 pm INTRODUCTION AND PROGRAM OVERVIEW

<u>Faculty:</u>

- **Andrew Grotto,** *William J. Perry International Security Fellow, Center for International Security and Cooperation (CISAC), Research Fellow, Hoover Institution*
- **Dr. Herb Lin,** *Senior Research Scholar, CISAC; Hank J. Holland Fellow, Hoover Institution*

12:00 pm – 12:30 pm LUNCH KEYNOTE & WELCOME

<u>Opening Remarks:</u>

H.R. McMaster, *Fouad and Michelle Ajami Senior Fellow, Hoover Institution; Former assistant to the president for National Security Affairs; Retired Lieutenant General, U.S. Army*

12:30 pm – 1:30 pm THINKING LIKE AN ATTACKER

<u>Faculty:</u>

- **Dr. Greg Conti,** *Senior Security Strategist, IronNet Cybersecurity*
- **Dr. Herb Lin,** *Stanford University*
- **Andrew Grotto,** *Stanford University (Moderator)*

Effectively combating any adversary requires understanding the ways in which that adversary thinks. Cybersecurity adversaries — from state agents seeking to disable military systems to hacktivists seeking to make a political point — share a security mindset: a predilection for examining the ways in which the security of a system can be circumvented or penetrated. Whereas good engineering is about how a system can be made to work, the security mindset involves thinking about how some aspect of a system can be made to fail. Understanding this mindset is the first step towards designing sound cybersecurity solutions.

<u>Assignment:</u> While in transit to the course location in Palo Alto, conduct a thought experiment for bringing an item prohibited by TSA regulations onto the airplane.

<u>Learning Objectives:</u> Why defense is more difficult than offense and what makes ongoing offense-defense competition inevitable.

1:30 pm – 1:45 pm BREAK

1:45 – 3:00 pm KEYNOTE: CURRENT THREAT LANDSCAPE

- **Kevin Mandia,** *CEO, FireEye*
- **Sean Kanuck,** *Visiting Fellow, Hoover Institution; Former National Intelligence Officer for Cyber Issues, Office of the Director of National Intelligence*
- **Dr. Herb Lin,** *Stanford University (Moderator)*

Threat actors and their specific activity signatures, global hot spots and trends, are analyzed daily by various security agencies, governments, and organizations. This keynote will direct our attention to today's principal threat actors, providing a bird's eye view of the threat landscape, current trends and capabilities, future outlook of malicious cyber activity, and seeks to bust certain myths sometimes circulated or recounted incorrectly about cyber operations. Speakers will also provide first-hand examples of experiences tracking threats and bad actors, and share insights about working in this field.

3:00 pm – 3:15 pm BREAK

3:15 pm – 4:15 pm THREATS TO CYBERSECURITY

<u>Faculty:</u>
- **Carey Nachenberg,** *Chief Scientist, Chronicle; Adjunct Assistant Professor of Computer Science, UCLA*
- **Dr. Tom Berson,** *Visiting Scholar, Stanford CISAC; Advisory Board Member, Salesforce; Founder, Anagram Laboratories*
- **Dr. Herb Lin,** *Stanford University (Moderator)*

Cybersecurity compromises can take a variety of forms and occur for a variety of reasons. This session examines various known techniques and vulnerabilities in information technology that allow them to happen, painting a picture of a well-known cybersecurity theme: offense

dominance. This session will include forensic case studies that illuminate the spectrum of the attack surface, key challenges, and trends.

Learning Objectives: Security-relevant principles of information technology; types of compromises; inherent vulnerabilities of information technology; the hidden complexity of cyberspace; anatomy of security compromises; and the spectrum of threats to cybersecurity.

4:15 pm – 4:30 pm BREAK

4:30 pm – 5:30 pm DINNER: OFFENSIVE DIMENSIONS OF CYBERSECURITY

Faculty:
- **Dr. Herb Lin,** *Stanford University*
- **Jason Kichen,** *Vice President, Advanced Security Concepts, eSentire*
- **Andrew Grotto,** *Stanford University (Moderator)*

Offensive activities — including those conducted for espionage and attack purposes — serve a variety of national goals. This discussion will summarize the operational and strategic requirements, intelligence needs, organizational structure and policy considerations necessary for offensive cyber operations.

Learning Objectives: The role of offensive operations in cyberspace for improving the nation's cybersecurity posture, signaling, and other purposes; the differences between penetration and exploitation and their important distinctions; the scope and nature of U.S. command and control of offensive operations in cyberspace.

5:30 pm – 6:00 pm BREAK

6:00 pm – 8:30 pm HOSPITAL RANSOMWARE SIMULATION

The hospital has been the victim of a cyber-attack in the form of ransomware which successfully encrypts 250,000 files and holds at least one system hostage, demanding a ransom payment in Bitcoin (BTC) in return for a decryption key which will unlock its systems and restore access and functionality to the system. The hospital has a timeline of 72 hours to pay the ransom before their files become permanently encrypted and inaccessible, or are moved off their network.

Subject matter experts will act as the hospital's Chief Executive Officer and Chief Strategy Officer during the simulation, and staffers will be divided into teams to assist with directing action items, press releases, and critical decisions on how to manage the attack and response. Each team will have a coach aiding their organization and strategy. All names and information will be fictional, however, the simulated attack is based on previous real life scenarios. The information made available to participants is subject to change throughout the simulation. At the end of the exercise, teams will present their decision making processes to the hospital's CEO and Board of Trustees, and debrief on what it is like to face this type of cyber scenario in the real world.

DAY 2 (Tuesday, August 27): Technical & Nontechnical Approaches

8:30 am – 9:00 am BREAKFAST AND DAY 1 DEBRIEF

- **Andrew Grotto,** William J. Perry International Security Fellow, Center for International Security and Cooperation (CISAC), Research Fellow, Hoover Institution
- **Dr. Herb Lin,** *Senior Research Scholar, CISAC; Hank J. Holland Fellow, Hoover Institution*

9:00 am – 11:00 am HANDS ON HACK LAB

<u>Faculty:</u>
- **Alex Stamos,** *Visiting Scholar, Hoover Institution; Adjunct Professor, Stanford University; Director, Internet Observatory, Cyber Policy Center, Freeman Spogli Institute*

Stamos' course provides an introduction to the most common types of attacks used in cybercrime and cyberwarfare. As a long-time security practitioner, he covers the basics of an area of technology and how it has been misused. Participants will complete a lab session from his Stanford course in which they will be guided through attacking a known insecure system using techniques and tools seen in the field.

Participants will be required to bring a Windows or Mac laptop and will be provided with basic information for the exercise 2 weeks prior to the session. No computer science background is necessary for this session.

11:00 am – 11:15 pm BREAK

11:15 am – 12:15 pm LUNCH: CYBER RISK, ECONOMICS, AND ORGANIZATIONAL DIMENSIONS OF CYBERSPACE

<u>Faculty:</u>
- **Dr. Tyler Moore,** *Tandy Assistant Professor of Cyber Security and Information Assurance, University of Tulsa*
- **Dr. Greg Falco,** *Security Researcher, Stanford CISAC*
- **Dr. Herb Lin,** *Stanford University (Moderator)*

Known cybersecurity measures are often not fully adopted due to a variety of economic and organizational factors. These factors are non-technical in nature and often underappreciated by technical and policy communities. Economics describe the incentives that apply to cyber defenders and adversaries, including the nature of cybersecurity market failures and the ability to handle collective action problems. The insurance sector is working to provide accurate and adequate coverage for this market. This session examines how these factors often discourage the adoption of sound security practices.

<u>Learning Objectives</u>: The importance of economic and organizational factors of cybersecurity and why they are often overlooked in efforts to improve cybersecurity; how government action might help to address non-technical factors that diminish the nation's cybersecurity posture.

12:15 pm – 12:30 pm BREAK

12:30 pm – 1:30 pm PRIVACY & SECURITY FOR CONSUMERS, CUSTOMERS, AND CRITICAL INFRASTRUCTURE

<u>Faculty:</u>
- **Robert Chesney,** *Associate Dean and Charles I. Francis Professor, University of Texas School of Law; Director, Robert S. Strauss Center for International Security and Law*
- **Ted Gizewski,** *Vice President, Product Legal, Salesforce*
- **Andrew Grotto,** *Stanford University (Moderator)*

Privacy and security risks manifest differently in different business sectors. They also share important interdependencies that require integrated risk management and policy-making strategies.

<u>Learning objectives</u>: Gaining insight into how privacy and security risks affect different sectors, how risk management strategies must be tailored to the risk environment, and why an integrated approach to managing privacy and security risks is imperative.

1:30 pm – 1:45 pm BREAK

1:45 pm – 2:45 pm INTERNATIONAL LAW AND CYBERSECURITY

<u>Faculty:</u>
- **Dr. Tess Bridgeman,** *Senior Fellow, Center on Law and Security, NYU*
- **Dr. Herb Lin,** *Stanford University*
- **Andrew Grotto,** *Stanford University (Moderator)*

Technological change has far outpaced updates to laws and regulatory frameworks, and will almost certainly continue to do so in the future. This lag consequentially challenges Congress to craft legislation appropriate for future technologies. Furthermore, nations have cooperative and competitive (and sometimes adversarial) interests that play out in cyberspace, devoid of national borders, giving an international dimension to every cybersecurity and policy challenge.

<u>Learning Objectives</u>: The implicit technological assumptions of existing cybersecurity laws; what problems arise in applying existing international law to technological circumstances not contemplated at the time of initial passage. These include the law of armed conflict, human rights, proposals for internet governance; and different non-governmental organizations that affect the design and operation of the Internet.

2:45 pm – 3:45 pm FUNDAMENTALS OF DEFENSE FOR CYBERSECURITY

<u>Faculty:</u>
> **Dr. Irving Lachow,** *Visiting Fellow, Hoover Institution; Affiliate, CISAC; Portfolio Manager, International Cybersecurity, MITRE*
> **Andrew Grotto,** *Stanford University*
- **Dr. Herb Lin,** *Stanford University (Moderator)*

Cybersecurity can be a deeply technical subject, especially in how cybersecurity solutions are implemented, a few fundamental principles underlie most solutions. This session takes a deep dive into the principles of improving cybersecurity and how they fit together. These include reducing reliance on information technology, detecting cybersecurity compromises, and

blocking and limiting the impact of compromise. Additional topics include authentication, access control, forensics, recovery, containment, resilience, and active defense.

Learning Objectives: The value of these fundamental principles of cybersecurity, understanding interdependencies, and how to use fundamentals and understanding collectively to improve security.

3:45 pm – 4:00 pm BREAK

4:00 pm – 5:00 pm CYBER ENABLED INFORMATION WARFARE AND INFLUENCE OPERATIONS

Faculty:
- **Dr. Rosanna Guadagno**, *Director, Information Warfare Working Group, Stanford University*
- **Dr. Herb Lin**, *Stanford University*
- **Andrew Grotto**, *Stanford University (Moderator)*

Cyber-enabled information warfare is fundamentally different than cyber war and cyber conflict, at least as the latter are generally understood today in the policy world. Cyber war and cyber conflict target information and information technology systems, whereas cyber-enabled information warfare targets human minds. Russia did not "hack" Facebook and YouTube and Twitter by penetrating their security—it used those platforms exactly as they were designed to be used. This session delves into these differences, placing the emphasis on the psychological vulnerabilities of people that the Russians (and other institutional users of social media) exploit for gain.

Learning Objectives: Understanding the fundamental differences between cyber war and cyber-enabled information warfare; the psychology underlying cyber-enabled information warfare; and the present inadequacies of the U.S. government in coping with such warfare.

5:00 pm – 6:30 pm BREAK

6:30 pm – 8:30 pm KEYNOTE RECEPTION/DINNER – ARTIFICIAL INTELLIGENCE

- **Dr. John Etchemendy,** *Co-Director, Stanford Institute for Human-Centered Artificial Intelligence; Provost Emeritus, and Patrick Suppes Family Professor in the School of Humanities, Stanford University*
- **Reid Hoffman,** *Co-founder and former Executive Chairman, LinkedIn*
- **Ambassador Michael McFaul,** *Senior Fellow, Freeman Spogli Institute for International Studies; Senior Fellow, Hoover Institution, Stanford University (Moderator)*

Artificial intelligence technologies are augmenting human capability and efficiency, changing the way we think about and interact with information, and creating new governance challenges and opportunities for policy makers and business leaders. Please join two distinguished thought leaders to discuss critical issues facing the future of human-centered AI development, innovation, and governance.

DAY 3 (Wednesday, August 28): Industry Voices, and the Future of Artificial Intelligence

---

9:00 am – 9:30 am BREAKFAST AND DAY 2 DEBRIEF

- **Andrew Grotto**, *William J. Perry International Security Fellow, Center for International Security and Cooperation (CISAC), Research Fellow, Hoover Institution*
- **Dr. Herb Lin**, *Senior Research Scholar, CISAC; Hank J. Holland Fellow, Hoover Institution*

9:30 am – 10:45 am INDUSTRY PERSPECTIVES PANEL

- **Dr. Sameer Bhalotra (Chair)**, *Co-Founder and CEO, ActZero.ai; Affiliate, CISAC; Senior Associate of the Strategic Technologies Program, CSIS; former Senior Director for Cybersecurity, National Security Council*
- **Frank Chen**, *Partner, Andreessen Horowitz*
- **Michelle Finneran Dennedy**, *Vice President, Chief Privacy Officer, Cisco*
- **Rick Howard**, *Chief Security Officer, Palo Alto Networks*
- **Dr. Mark Rosekind**, *Chief Safety Innovation Officer, Zoox*

Market forces have a critical role in enhancing or weakening security and privacy considerations. This session examines how such forces play out at the level of the individual firm and incorporate the views and concerns of the business community. Silicon Valley senior executives and engineers will give their "ground truths" about the security problems facing the private sector.

<u>Learning Objectives</u>: Various private sector perspectives on technology and relations beyond Silicon Valley from technology firms that support innovative efforts for providing IT-based products and services with attention to cybersecurity and AI.

10:45 am – 11:00 am BREAK

11:00 am – 12:00 pm FUNDAMENTALS OF AI AND MACHINE LEARNING

Faculty:

- **Dr. Emma Brunskill,** *Assistant Professor, Computer Science, Stanford University; Stanford AI for Human Impact Lab*
- **Dr. Jeff Clune,** *Harris Associate Professor, Computer Science, University of Wyoming; Senior Research Manager, Uber AI Labs*
- **Andrew Grotto,** *Stanford University, (Moderator)*

Machine learning and the algorithms that fuel its applications have important principle foundations including deep learning neural networks, increased complexity in evolving neural networks, and robotics developments which are increasingly intelligent, adaptable, and resilient. Also known as reinforcement learning, algorithms can learn from experience to make decisions or provide diagnostics in applications such as educational software, healthcare decision making, robotics, or people-facing applications. This session will explain the basic elements of machine learning, and the typical environment for building and testing neural networks and reinforcement learning.

Learning Objectives: Practical applications and limits of machine learning, the broad strokes of development of deep neural networks, and the overall veracity of both development and applications of this technology. Faculty will also speak to the trajectory of the technology, and any risks it may pose from a technical perspective.

12:15 pm – 1:15 pm KEYNOTE LUNCH: ARTIFICIAL INTELLIGENCE AND SAFETY

- **Dr. Fei-Fei Li,** *Co-Director, Stanford Human-Centered Artificial Intelligence Initiative, Stanford University; Professor, Computer Science, Stanford University*
- **Mykel Kochenderfer,** *Assistant Professor of Aeronautics and Astronautics, Stanford University; Director, Stanford Intelligent Systems Laboratory*
- **Andrew Grotto,** *Stanford University (Moderator)*

Building robust decision making systems is challenging, especially for safety critical systems such as unmanned aircraft and driverless cars. Decisions must be made based on imperfect information about the environment and with uncertainty about how the environment will evolve. In addition, these systems must carefully balance safety with other considerations, such as operational efficiency. Typically, the space of edge cases is vast, placing a large burden on human designers to anticipate problem scenarios and develop ways to resolve them.

Learning Objectives: We will discuss ways in which artificial intelligence can be applied to the design of these safety critical systems. This approach has the potential to significantly improve robustness of these systems, but there are two major challenges. The first is in ensuring computational tractability, and the other is establishing trust in their correct operation when deployed in the real world. We will outline some methodologies for addressing these challenges.

1:15 pm – 1:30 pm BREAK

1:30 pm – 2:30 pm ETHICS AND GOVERNANCE FOR AI

<u>Faculty:</u>

- **Dr. John Villasenor,** *Visiting Fellow, Hoover Institution; Professor of Electrical Engineering, Law, Public Policy, and Management, University of California Los Angeles*
- **Dr. Patrick Lin,** *Director, Emerging Sciences Group, California Polytechnic State University*
- **Dr. Herb Lin, Stanford** *University (Moderator)*

Advances in AI are raising a set of fundamentally important questions that go well beyond technology. This session will explore key AI ethics and governance issues, such as the nuances and challenges of addressing questions like: What should the rules be when machines make decisions with ethical implications, and who writes those rules? How can the issue of bias in AI be addressed?

Learning Objectives: The sorts of governance structures that can best ensure a climate of innovation in the AI ecosystem while also protecting against its potential misuses. What special issues are raised by AI in defense and security specifically.

2:40 pm – 3:50 pm HOOVER TOWER AND ARCHIVES TOUR

Founded by Herbert Hoover in 1919, the Hoover Institution Library & Archives are dedicated to documenting war, revolution, and peace in the twentieth and twenty-first centuries. With nearly one million volumes and more than six thousand archival collections from 171 countries, Hoover supports a vibrant community of scholars and a broad public interest in the meaning and role of history.

4:15 pm – 5:30 pm VISIT TO CENTER FOR AUTOMOTIVE RESEARCH AT STANFORD

Faculty:

- **Dr. Stephen Zoepf,** *Executive Director, Center for Automotive Research,*
  Stanford University
  Bryan Casey, *Lecturer in Law, Stanford University*
  Marco Pavone, *Associate Professor, Aeronautics and Astronautics,*
  Stanford University

The Center for Automotive Research at Stanford (CARS) brings together researchers, students, industry, government and the community to enable a future of human-centered mobility. Understanding how people and machines work together has never been so important than when building vehicles of the future. CARS supports educational experiences for students, infrastructure for research and events that bring students and campus researchers together with industry professionals and the broader community. Researchers and vehicles affiliated with CARS are housed at the Automotive Innovation Facility, which houses the Volkswagen Automotive Innovation Lab (often referred to as 'VAIL'), a state-of-the-art vehicle research facility where interdisciplinary teams can work on projects that move vehicle human-centered mobility forward.

Participants will visit CARS' Automotive Innovation Facility and hear from researchers on the cutting edge of the development of autonomous vehicles. Experts will brief the group on trends in the field, ongoing legal and ethical debates, and provide a tour of the facility showcasing vehicles and a driving simulator used for research.

6:00 pm – 8:00 pm DINNER AND REFLECTIONS

Coupa Café
198 Junipero Serra Blvd, Stanford, CA, 94305

Thursday, August 29

9:30 a.m. - Privately sponsored trip formally ends. Clint Trocchio has extended his trip and will return on August 31st to Washington, DC.